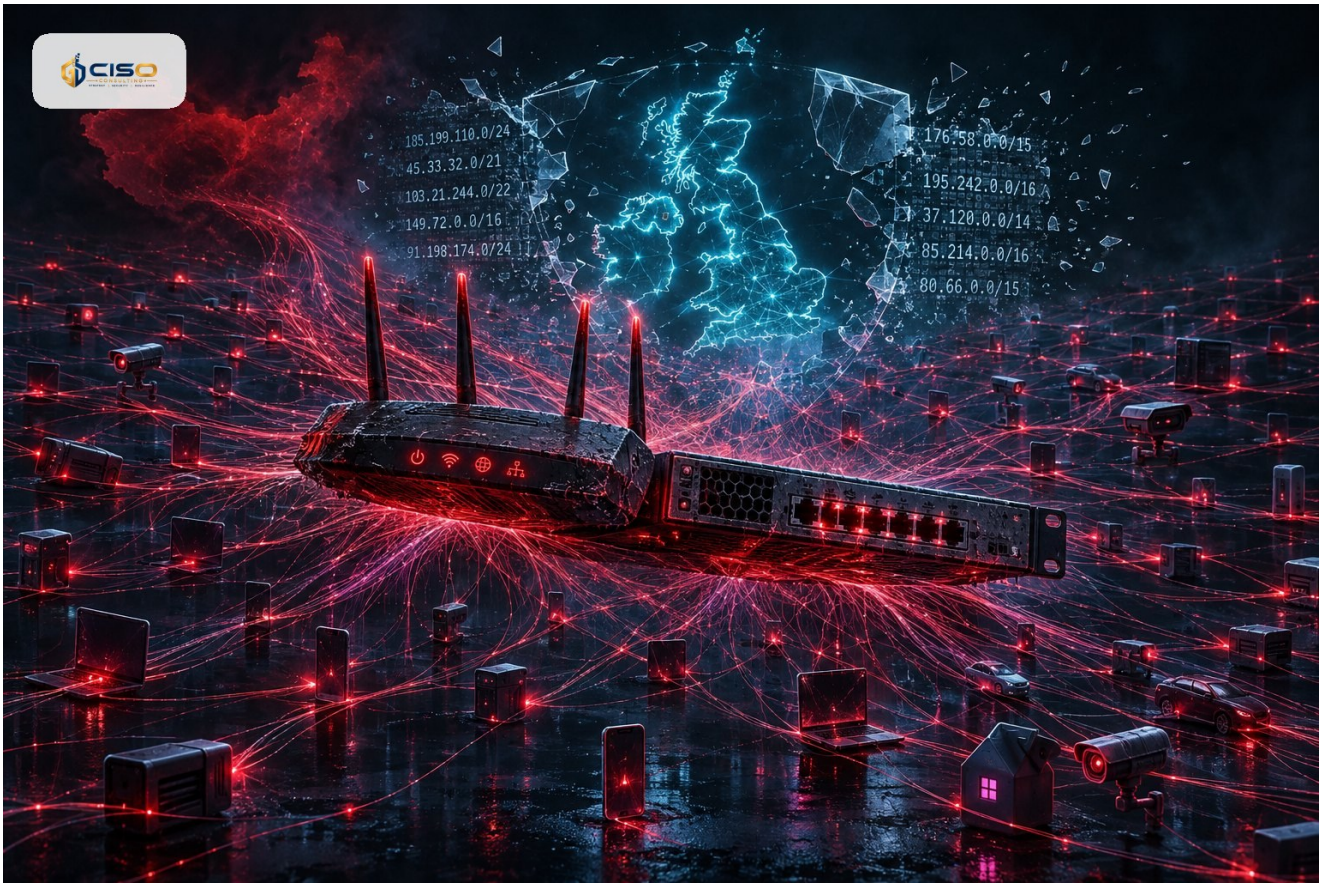
NCSC advisory: China-nexus actors use covert networks of compromised edge devices



The UK NCSC and partner agencies warn that China-nexus actors now run botnets of compromised routers and edge devices, making static IP block lists ineffective. The advisory sets out mapping, baselining and zero trust steps.

- China-nexus actors have shifted from individually procured infrastructure to large covert networks built from compromised routers and other edge devices.
- The networks support every phase of the kill chain, from reconnaissance to data exfiltration.
- Nodes are constantly refreshed and shared across threat groups, so indicators of compromise expire as fast as they are found.
- Organisations relying only on static defences risk being bypassed.
- The advisory gives separate guidance for small, medium and large organisations.

The UK National Cyber Security Centre (NCSC), together with the Cyber League and co-sealing agencies, has published an advisory on a change in how China-nexus cyber actors build their attack infrastructure. Instead of procuring servers individually, they increasingly operate large covert networks: botnets made of compromised routers and other edge devices.

What the threat looks like

These networks are used at every stage of an intrusion, including reconnaissance, malware delivery, command and control, and data exfiltration. They are described as low-cost, deniable and quick to reshape, which makes traditional static IP block lists ineffective.

Because the networks are refreshed constantly and their nodes are shared among several threat groups, defenders face what the NCSC calls "IOC extinction": indicators of compromise vanish as quickly as they are discovered. The stated impact is theft of sensitive data and possible disruption of critical services.

What the advisory recommends

Guidance is provided for small, medium and large organisations. For all organisations:

- Map and baseline edge device traffic, especially VPN and remote access connections.
- Adopt dynamic threat feed filtering that includes known covert network indicators.

Potential victims should add two-factor authentication for remote access and, where possible, zero trust controls, IP allow lists and machine certificate verification. Larger or high-risk entities should consider active hunting for suspicious SOHO and IoT traffic, geographic profiling and machine learning based anomaly detection.

The NCSC concludes that prompt application of mapping, baselining and zero trust measures is essential to reduce exposure. The source does not mention Saudi-specific targeting.

What to do now

1. Inventory edge devices (routers, VPN and remote access gateways) and baseline their normal traffic.
2. Enforce multi-factor authentication on all remote access and VPN services.
3. Replace reliance on static IP block lists with dynamic threat feed filtering that is updated continuously.
4. Where feasible, apply IP allow lists, machine certificate verification and zero trust access to remote connections.
5. For large or high-risk entities, assess hunting of SOHO/IoT traffic and anomaly detection for edge traffic.
6. Review the full NCSC advisory and align it with existing NCA ECC and SAMA CSF controls.